UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,119	12/22/2003	W. Carey Bunn	END920030045US1(IBME.003P	7503

7590 03/28/2007

Arthur J. Samodovitz
IBM Corporation, Dept 1QOA/Bldg. 40-3
1701 North Street
Endicott, NY 13760

EXAMINER	
SCHMIDT, KARI L	
ART UNIT	**PAPER NUMBER**
2139	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/743,119	BUNN ET AL.	
	Examiner	Art Unit	
	Kari L. Schmidt	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/22/2003 & 1/19/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-11 are rejected under 35 U.S.C. 102(b) as being anticipated by Cisco System "Network Security: An Executive Overview".

Claim 1

Cisco System discloses a method for checking network perimeter security, said method comprising the steps of:

reviewing security of a network perimeter architecture (page 4: "Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass through the network");

reviewing security of data processing devices that transfer data across the perimeter of the network (page 4: Perimeter security: a firewall provides a barrier to traffic crossing a network's "perimeter" and permits only authorized traffic to pass, according to a predefined security policy");

reviewing security of applications that transfer data across said perimeter (page 4: Perimeter security: a firewall provides a barrier to traffic crossing a network's "perimeter" and permits only authorized traffic to pass, according to a predefined security policy");

and

reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (page 4: "Security monitoring: intrusion detection systems and vulnerability scanners provide an additional layer of network security. The system uses sensors, which are high-speed network appliances, to analyze individual packets to detect suspicious activity. If the data stream in a network exhibits unauthorized activity or a network attack, the sensors can detect the misuse in real time, forward alarms to an administrator and remove the offender from the network").

Claim 2

Cisco System discloses the method as set forth in claim 1 further comprising the step of reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter (page 3: "Identity: identity is the accurate and positive identification of network users, hosts, applications, services and resources. Cisco Secure Access Control Server to provide a foundation that authenticates user, determines access levels and archives all necessary audit and accounting data").

Claim 3

Cisco System discloses the method as set forth in claim 1 further comprising the step of reviewing security of data processing devices that authorize computers or users outside

of said perimeter that request to access an application within said perimeter (page 3: "Identity: identity is the accurate and positive identification of network users, hosts, applications, services and resources. Cisco Secure Access Control Server to provide a foundation that authenticates user, determines access levels and archives all necessary audit and accounting data").

Claim 4

Cisco System discloses the method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of a web server, an e-mail server or an FTP server (page 2: Cost of Intrusion: "web server = e-commerce web sites; and email systems and using AAA capabilities of the Cisco Secure Access Control Server to provide foundation that authenticates users, determines access levels and archives all necessary audit and accounting data on page 4").

Claim 5

Cisco System discloses the method as set forth in claim 1 further comprising the step of reviewing security of a server within said perimeter that provides data to said data processing devices that transfer data across the perimeter of said network (page 4: "using AAA capabilities of the Cisco Secure Access Control Server to provide foundation that authenticates users, determines access levels and archives all

necessary audit and accounting data").

Claim 6

Cisco System discloses the method as set forth in claim 1 wherein each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls said network (page 3: Designing the security infrastructure: "enterprises should make sure to consider their network security implementations as competitive advantages that can attract customers, employees, and partners; security architecture integrated into the existing enterprise network and on page 4: Cisco Secure Policy Manager supports Cisco security elements in enterprise networks, ensuring a comprehensive, consistent implementation of security policy").

Claim 7

Cisco System discloses the method as set forth in claim 1 further comprising the step of determining said network perimeter (page 4: Perimeter Security: "control access/determine access to critical network applications, data and services so that only legitimate users and information can pass through the network" and Secure Connectivity).

Claim 8

Cisco System discloses the method as set forth in claim 7 wherein said network perimeter comprises entries and exits from said network (page 4: Perimeter Security:

"control access to critical network applications, data and services so that only legitimate users and information can pass (enter and exit) through the network").

Claim 9

Cisco System discloses the method as set forth in claim 1 wherein said network perimeter comprises entries and exits from said network (page 4: Perimeter Security: "control access to critical network applications, data and services so that only legitimate users and information can pass (enter and exit) through the network").

Claim 10

Cisco System discloses the method as set forth in claim 1 wherein the steps of reviewing security of a network perimeter architecture (page 4: "Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass through the network"), reviewing security of data processing devices that transfer data across the perimeter of the network (page 4: Perimeter security: a firewall provides a barrier to traffic crossing a network's "perimeter" and permits only authorized traffic to pass, according to a predefined security policy"), and reviewing vulnerability of applications or data processing devices within said perimeter from entities outside of said perimeter are performed at least in part with a respective program tool (page 4: "Security monitoring: intrusion detection systems and vulnerability scanners provide an additional layer of network security. The system uses sensors, which are high-speed network appliances, to analyze individual packets to

detect suspicious activity. If the data stream in a network exhibits unauthorized activity or a network attack, the sensors can detect the misuse in real time, forward alarms to an administrator and remove the offender from the network" and Security Monitor: " Cisco Scanner is an enterprise-class software and page 5: SAFE blueprint").

Claim 11

Cisco System discloses the method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of data processing devices accessed by users outside of said perimeter (page 3: "Identity: identity is the accurate and positive identification of network users, hosts, applications, services and resources. Cisco Secure Access Control Server to provide a foundation that authenticates user, determines access levels and archives all necessary audit and accounting data").

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Wiegel (US 6, 484, 261 B1) teaches a method of establishing a representation of a network security policy and controls a network device that passes or rejects information messages.

Kurtz et al. (US 2003/0217039 A1) teaches a system and method provide comprehensive and highly automated testing of vulnerabilities to intrusion on a target network.

Currie et al. (US 2005/0160286 A1) teaches security verification of the security status of online services.

eSoft (http://www.kfa-inc.com/techtips/securitywhitepaper.pdf) teaches overview of network security threats and how they are typically managed and proposes an improved, simplified approach that can be achieved through the integration of security technologies.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kari L. Schmidt whose telephone number is 571-270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS

Jagdish J. Patel
Primary Examiner
3/26/07